Title (en)

TECHNIQUE FOR REDUCING RSA CRYPTO VARIABLE STORAGE

Publication

**EP 0202768 B1 19920715 (EN)**

Application

**EP 86302861 A 19860416**

Priority

US 72871785 A 19850430

Abstract (en)

[origin: EP0202768A2] A technique for reducing RSA (Rivest, Shamir and Adleman algorithm) cryptovariable key from 1200 bits (400-bit public key, 400-bit secret key and 400-bit modulus) to 106 bits makes feasible the storage of the RSA algorithm parameters on current magnetic stripe cards used by the banking and finance industry. Of the 106 bits required, only 56 bits must be kept secret; the remaining 50 bits are nonsecret. These 106 bits are used to derive two 200-bit primes P and Q from which is computed the modulus N = PQ and two 400-bit keys PK (public key) and SK (secret key). In effect, a savings in storage is achieved at the expense of performing a precomputation to derive the modulus an keys each time the system is utilised for encryption/decryption. The 56-bit value plus the additional 50 bits of nonsecret data can be used to generate the RSA cryptovariables in systems where the RSA algorithm has been implemented. In another embodiment, a technique is provided for reducing the RSA cryptovariable storage of the public key PK and modulus from 800 bits to 242 bits. These 242 bits can be used at any later time to derive the 400-bit public key PK and 40--bit modulus N = PQ. The savings in storage is achieved by performing a precomputation each time the system is utilised for encryption/decryption.

IPC 1-7

G07F 7/10; H04L 9/00

IPC 8 full level

**G07F 7/10** (2006.01); **H04L 9/30** (2006.01)

CPC (source: EP US)

**G07F 7/1016** (2013.01 - EP US); **H04L 9/302** (2013.01 - EP US); **H04L 9/3226** (2013.01 - EP US); H04L 2209/26 (2013.01 - EP US); H04L 2209/56 (2013.01 - EP US)

Cited by

EP1043654A3; EP0325238A3; US6473743B1; EP0534420A3; FR2830146A1; GB2264423A; GB2264423B; EP0566512A1; FR2690258A1; US6952476B1; US7142668B1; US7386123B2; WO03028286A1

Designated contracting state (EPC)

DE FR GB

DOCDB simple family (publication)

**EP 0202768 A2 19861126**; **EP 0202768 A3 19881109**; **EP 0202768 B1 19920715**; DE 3685987 D1 19920820; DE 3685987 T2 19930204; US 4736423 A 19880405

DOCDB simple family (application)

**EP 86302861 A 19860416**; DE 3685987 T 19860416; US 82315186 A 19860131